

USDC SDNY
DOCUMENT
ELECTRONICALLY FILED
DOC #:
DATE FILED: 10/4/2017

-----X		DOC #:
	:	DATE FILED: <u>10/4/2017</u>
JESSIE SACKIN, et al.,	:	
	:	
Plaintiffs,	:	
	:	17 Civ. 1469 (LGS)
-against-	:	
	:	
TRANSPERFECT GLOBAL, INC.,	:	<u>OPINION AND ORDER</u>
Defendant.	:	
	:	
-----X		

Plaintiffs filed this purported class action against TransPerfect Global, Inc.

(“TransPerfect” or “Defendant”) on February 27, 2017, stemming from a data breach of TransPerfect’s computer systems that disclosed Plaintiffs’ sensitive personally identifiable information (“PII”) to hackers. TransPerfect moves to dismiss the Amended Complaint (“Complaint”) pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). As discussed below, the Rule 12(b)(1) motion is denied because Plaintiff has standing to sue. The Rule 12(b)(6) motion is granted in part, dismissing only the claim of breach of express contract.

The following facts are drawn from the Complaint and accepted as true for the purpose of this motion. Defendant employs over 4,000 individuals. The company maintains a corporate privacy policy and security manual that describes “robust procedures designed to protect the PII with which it is entrusted.” However, unlike other similarly situated companies, TransPerfect did not train employees on data security; did not erect digital firewalls and did not maintain PII retention and destruction protocols.

Defendant understood the prevalence of cyber-attacks on corporate records and

appreciated the gravity of the risk posed by such attacks. High-profile corporate data breaches dominated recent headlines, and 282 breaches were publicly reported between 2014 and 2015. Defendant's own website warns clients that cyber-attacks "are neither new nor infrequent." The website cautions, "never send your credit card number, Social Security number, bank account number, driver's license number or similar details in an email," because email "is generally not secure" and is the method of communication "most vulnerable to hacking."

On or about January 17, 2017, at least one TransPerfect employee received a "phishing" email. The email appeared to come from TransPerfect's CEO, but actually was sent by unidentified cyber-criminals. The email asked for the W-2 forms and payroll information of all current and former TransPerfect employees. Because TransPerfect's cyber-security was not up to industry par, at least one TransPerfect employee sent the information to the hackers in an unencrypted format. As a result, cyber-criminals obtained Plaintiffs' names, addresses, dates of birth, Social Security numbers, direct deposit bank account numbers and routing numbers.

Hackers can use PII to obtain by fraud employment, loans, credit cards and can file tax returns. Criminals can also use PII to steal government benefits and create false identification for use in further schemes. Stolen PII is frequently bought and sold amongst various criminals on "dark markets." TransPerfect responded to the breach by offering Plaintiffs two free years of enrollment in an identity theft *monitoring* service. Plaintiffs purchased *preventive* services.

II. LEGAL STANDARDS

"A district court properly dismisses an action under Fed. R. Civ. P. 12(b)(1) for lack of subject matter jurisdiction if the court lacks the statutory or constitutional power to adjudicate it, such as when . . . the plaintiff lacks constitutional standing to bring the action." *Cortlandt St. Recovery Corp. v. Hellas Telecomms., S.A.R.L.*, 790 F.3d 411, 416–17 (2d Cir. 2015) (internal

citation omitted). The task of the district court is to determine whether the “[p]leading allege[s] facts that affirmatively and plausibly suggest that [the plaintiff] has standing to sue.” *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 56 (2d Cir. 2016) (internal quotation marks omitted). “In resolving a motion to dismiss under Rule 12(b)(1), the district court must take all uncontroverted facts in the complaint . . . as true, and draw all reasonable inferences in favor of the party asserting jurisdiction.” *Fountain v. Karim*, 838 F.3d 129, 134 (2d Cir. 2016) (quoting *Tandon v. Captain’s Cove Marina of Bridgeport, Inc.*, 752 F.3d 239, 243 (2d Cir. 2014)). “The plaintiff bears the burden of alleging facts that affirmatively and plausibly suggest that it has standing to sue.” *Cortland*, 790 F.3d at 417 (internal quotation marks omitted). The issue of subject matter jurisdiction is resolved before turning to the sufficiency of the Complaint. *See generally Carver v. Nassau Cty. Interim Fin. Auth.*, 730 F.3d 150, 156 (2d Cir. 2013) (“Normally, in cases involving the issue of Article III subject matter jurisdiction, this issue would have to be addressed first.”).

To survive a motion to dismiss under Rule 12(b)(6), “a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Id.* On a Rule 12(b)(6) motion, “all factual allegations in the complaint are accepted as true and all inferences are drawn in the plaintiff’s favor.” *Littlejohn v. City of N.Y.*, 795 F.3d 297, 306 (2d Cir. 2015).

III. DISCUSSION

A. Subject Matter Jurisdiction

The motion to dismiss for lack of subject matter jurisdiction is denied because the

Complaint “affirmatively and plausibly” alleges facts sufficient to establish standing. *See HealthPort Techs.*, 822 F.3d at 56. The Complaint alleges four injuries as a consequence of the data breach: (1) an imminent risk of future identity theft; (2) lost time and money expended to mitigate the threat of identity theft; (3) diminished value of personal information; and (4) a loss of privacy. Because the first and second alleged harms satisfy constitutional standing requirements, this opinion does not address the other two claimed injuries.

“[T]he irreducible constitutional minimum of standing contains three elements.” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). “The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” *Spokeo, Inc. v Robins*, 136 S. Ct. 1540, 1547 (2016) (internal quotation marks and citation omitted). Defendant challenges only the first element, arguing that the Complaint does not plead injury in fact. As explained below, this argument is incorrect.

To satisfy the injury-in-fact requirement, a plaintiff must allege “an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical.” *John v. Whole Foods Mkt. Grp.*, 858 F.3d 732, 736 (2d Cir. 2017) (citing *Spokeo*, 136 S. Ct. at 1548). Allegations of future harm establish injury in fact as long as the future harm is “certainly impending.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409 (2013). By contrast, mere “[a]llegations of possible future injury are not sufficient.” *Id.* (internal quotation marks omitted). While “imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes” *Id.*

The harms alleged in the Complaint do not stretch imminence beyond its breaking point. The allegations that Defendant has provided Plaintiffs' names, addresses, dates of birth, Social Security numbers and bank account information directly to cyber-criminals creates a risk of identity theft sufficiently acute so as to fall comfortably into the category of "certainly impending." The most likely and obvious motivation for the hacking is to use Plaintiffs' PII nefariously or sell it to someone who would. *See Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."). Circuit courts addressing this issue consistently have held that Article III does not require Plaintiffs to wait for their identities to be stolen before seeking legal recourse. *See Attias v. Carefirst, Inc.*, 865 F.3d 620, at 629–30 (D.C. Cir. 2017) (holding that alleged increased risk of identity theft was sufficiently imminent to establish standing after a retailer's data breach); *Remijas*, 794 F.3d at 695 (same); *Galaria v. Nationwide Mut. Ins.*, 663 F. App'x 384, 388 (6th Cir. Sept. 12, 2016) (same); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 164 (1st Cir. 2011) (same).

While the Second Circuit has yet to address the question, two recent unreported decisions suggest that it will follow the lead of its sister circuits. *See Katz v. Donna Karan Co.*, --- F.3d ---, 2017 WL 4126942, at *5 (2d Cir. Sept. 19, 2017); *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. May 2, 2017) (summary order). In *Whalen*, the Second Circuit concluded that the complaint failed to allege standing because the plaintiff never paid a fraudulent charge, nor did she face a plausible threat of future harm. Her "stolen credit card was promptly canceled after the breach and no other personally identifying information -- such as her birth date or Social Security number -- is alleged to have been stolen." *Id.* Similarly, in *Katz*, the Second Circuit

held that a “district court did not clearly err in finding that the bare procedural violation in question [i.e., printing the last six digits of a customer’s credit card number on their store receipt] did not raise a material risk of harm of identity theft.” 2017 WL 4126942, at *6.

Whether the risk of identity theft is sufficiently material to create an injury in fact is “a question for lower courts to determine in the first instance, on a case- and fact-specific basis.” *Id.* Here, a case-specific analysis dictates that standing exists. The Complaint alleges that Defendant divulged information -- including birth dates and social security numbers -- far more sensitive than all or a portion of a credit card number, and that the PII here was provided directly to cybercriminals, and not merely printed on a store receipt.

When a future harm is sufficiently imminent to support standing, a plaintiff’s expenses in taking reasonable measures to prevent the harm’s fruition also may be viewed as an injury in fact. *See Hedges v. Obama*, 724 F.3d 170, 196 (2d Cir. 2013) (the Supreme Court has “sometimes found standing to sue where plaintiffs showed only a substantial risk that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm”) (quoting *Clapper*, 568 U.S. 398, 414 n.5 (2013)); *Nationwide Mut. Ins.*, 663 F. App’x at 388 (stating that, “Plaintiffs’ allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage”). Here, the Complaint alleges that Plaintiffs reasonably incurred the cost identity theft prevention services. Accordingly, the Complaint sufficiently alleges injury in fact, both regarding the risk of identity theft and remedial measures.

In an effort to circumvent the appellate decisions cited above, Defendant cites a handful of distinguishable cases in which courts found standing to be lacking when a plaintiff’s PII was on a stolen computer, and the plaintiffs did not allege or could not show that obtaining their PII

was the motivation for the theft. *See, e.g., Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017) (stating that “plaintiffs have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information”). Similarly inapt are cases where the stolen PII was significantly less sensitive -- and less useful to thieves -- than the Social Security numbers and banking information taken here. *See, e.g., Alonso v. Blue Sky Resorts, LLC*, 179 F. Supp. 3d 857, 862 (S.D. Ind. 2016) (no standing existed where “[o]nly names, credit card numbers, and card expiration dates were stolen . . .”).

As the allegations of the risk of identity theft and related mitigating expenses are sufficient to allege injury in fact and thereby confer standing, the Court has subject matter jurisdiction. The motion to dismiss based on Rule 12(b)(1) is denied.

B. Failure to State a Claim

The Complaint pleads five causes of action: (1) common law and statutory negligence; (2) breach of express contract; (3) breach of implied contract; (4) unjust enrichment and (5) violations of N.Y. Labor Law 203-d.¹ Defendant’s motion to dismiss the express contract claim is granted, but its motion to dismiss the other claims is denied.

1. Negligence

“Under New York law, in order to recover on a claim for negligence, a plaintiff must show (1) the existence of a duty on defendant’s part as to plaintiff; (2) a breach of this duty; and (3) injury to the plaintiff as a result thereof.” *Caronia v. Philip Morris USA, Inc.*, 715 F.3d 417,

¹ New York law applies as the parties assume that it does. “The parties’ briefs assume that [New York] state law governs this case, and ‘such implied consent is ... sufficient to establish the applicable choice of law.’” *Trikona Advisers Ltd. v. Chugh*, 846 F.3d 22, 31 (2d Cir. 2017) (quoting *Arch Ins. Co. v. Precision Stone, Inc.*, 584 F.3d 33, 39 (2d Cir. 2009)).

428 (2d Cir. 2013) (internal quotation marks omitted). The Complaint sufficiently alleges that TransPerfect breached a duty owed to Plaintiffs under both common law and negligence per se principles, and that Plaintiffs suffered injury as a result.

a) Breach of Common law Duty

The Complaint alleges a cognizable legal duty -- that Defendants had a duty to safeguard Plaintiffs' and class members' PII. "The definition and scope of an alleged tortfeasor's duty owed to a plaintiff is a question of law." *Pasternack v Lab. Corp. of Am. Holdings*, 59 N.E.3d 485, 490 (N.Y. 2016). In making that determination, "the court must settle upon the most reasonable allocation of risks, burdens and costs among the parties and within society, accounting for the economic impact of a duty, pertinent scientific information, the relationship between the parties, the identity of the person or entity best positioned to avoid the harm in question, the public policy served by the presence or absence of a duty and the logical basis of a duty" *In re N.Y. City Asbestos Litig.*, 59 N.E.3d 458, *8 (N.Y. 2016). "Foreseeability defines the scope of a duty once it has been recognized." *Id.* at *9.

Applying these factors, employers have a duty to take reasonable precautions to protect the PII that they require from employees. Employees ordinarily have no means to protect that information in the hands of the employer, nor is withholding their PII a realistic option. The employer is "best positioned to avoid the harm in question" *Id.* at *8. *See also Katz v. United Synagogue of Conservative Judaism*, 23 N.Y.S.3d 183, 184 (1st Dep't 2016) ("The parties' relationship may create a duty where it 'places the defendant in the best position to protect against the risk of harm and the specter of limitless liability is not present.'"). Employees -- much more than employers -- suffer the harmful consequences of a data breach of the employer. Potential liability in the absence of reasonable care provides employers with an

economic incentive to act reasonably in protecting employee PII from the threat of cyberattack.

The Complaint also sufficiently alleges that TransPerfect violated its duty to take reasonable steps to protect its employees' PII. The Complaint alleges that TransPerfect was aware of the sensitivity of PII and the need to protect it; TransPerfect's website warns, "never send . . . credit card number[s], Social Security number[s], bank account number[s] . . . or similar details in an email," because email "is generally not secure" and is "vulnerable to hacking." The Complaint also alleges that, despite this knowledge, Defendant failed to take reasonable steps to prevent the wrongful dissemination of Plaintiffs' PII -- including erecting a digital firewall, conducting data security training and adopting retention and destruction policies -- such that a TransPerfect employee responded to a phishing email by sending Plaintiffs' PII to cyber-criminals. These allegations are sufficient to state a claim for negligence.

b) Breach of Statutory Duty

The Complaint sufficiently alleges negligence *per se*. "Under the rule of negligence *per se*, if (1) a statute is designed to protect a class of persons, (2) in which the plaintiff is included, (3) from the type of harm which in fact occurred as a result of its violation, the issues of the defendant's duty of care to the plaintiff and the defendant's breach of that duty are conclusively established upon proof that the statute was violated." *German by German v. Fed. Home Loan Mortg. Corp.*, 896 F. Supp. 1385, 1396 (S.D.N.Y. 1995) (numbering added) (citing *Martin v. Herzog*, 126 N.E. 814 (N.Y. 1920)); PROSSER AND KEETON ON THE LAW OF TORTS, at 229–30 (5th ed. 1984); accord *Jordan v. Tucker, Albin & Assocs.*, No. 13 civ. 6863, 2017 WL 2223918, at *12 (E.D.N.Y. May 19, 2017).

The Complaint sufficiently alleges breach of a statutory duty. First, New York Labor Law makes it illegal for an employer to "communicate an employee's personal identifying

information to the general public.” N.Y. LAB. LAW § 203-d(1)(d) (McKinney 2009). The statute defines “personal identifying information” to include: the employee’s “social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent’s surname prior to marriage, or drivers’ license number.” *Id.* § 203-d(1)(c). Second, Plaintiffs are within the class of persons -- employees -- the law is designed to protect. Third, exposure of PII is precisely the harm that the statute seeks to prevent. Even the alleged method of Defendant’s breach is contemplated by the statute, which states, “It shall be presumptive evidence that a violation . . . was knowing if the employer has not put in place policies or procedures to safeguard against” the disclosure of PII. *Id.* § 203-d(3).

c) Injury

Defendant’s 12(b)(6) motion is somewhat duplicative of its 12(b)(1) motion, because both rely heavily on a claimed lack of injury. Defendant argues that the negligence claim is deficient because “Plaintiff does not properly plead that he suffered any actual cognizable injury.” This argument is unpersuasive; the Complaint sufficiently alleges injuries stemming from Defendant’s breach of duty.

As discussed above, the Complaint adequately alleges that Plaintiffs face an imminent threat of identity theft and have purchased preventive services to mitigate the threat. These mitigation expenses satisfy the injury requirements of negligence; otherwise Plaintiffs would face an untenable Catch-22. Under New York’s “doctrine of avoidable consequences,” a plaintiff must “minimize damages” caused by a defendant’s tortious conduct, and can recover mitigation costs for any “action [] reasonable under the circumstances” *Revelations Perfume & Cosmetics, Inc. v. Nelson*, No. 603350/2008, 2012 WL 1434856, at *3 (N.Y. Sup. Ct. Apr. 12, 2012) (citing *Fed. Ins. Co v. Sabine Towing & Transp. Co.*, 783 F.2d 347, 350–51 (2d

Cir.1986)). Accordingly, Plaintiffs were required to take reasonable steps to mitigate the consequences of the data breach; they could not passively wait for their identities and money to be stolen. The Complaint sufficiently alleges that Plaintiffs have taken such reasonable steps, and that they are entitled to reimbursement.

The economic loss rule -- which in the “absence of any personal injury or property damage precludes plaintiffs' claims for economic injury” in negligence cases -- does not bar Plaintiffs’ negligence claim, as Defendant suggests, for two reasons. *532 Madison Ave. Gourmet Foods, Inc. v. Finlandia Ctr., Inc.*, 750 N.E.2d 1097, 1101 (N.Y. 2001). First, the rule is inapplicable because the Complaint does not allege a products liability claim. *See Id.* at 1101 n.1 (stating that the economic loss rule “stands for the proposition that an end-purchaser of a product is limited to contract remedies and may not seek damages in tort for economic loss against a manufacturer”); *Travelers Cas. & Sur. Co. v. Dormitory Auth.-State N.Y.*, 734 F. Supp. 2d 368, 378 (S.D.N.Y. 2010). Second, despite the economic loss rule, “[a] negligence claim may be brought provided that the plaintiff alleges that ‘a legal duty independent of the contract itself has been violated.’” *Emerald Town Car of Pearl River, LLC v. Phila. Indem. Ins. Co.*, No. 16 Civ. 1099, 2017 WL 1383773, at *4 (S.D.N.Y. Apr. 12, 2017) (citing *Dorking Genetics v. United States*, 76 F.3d 1261, 1269 (2d Cir. 1996)). Also, as detailed above, the Complaint alleges breach of common law and statutory duties distinct from Defendant’s contractual duties. TransPerfect’s motion to dismiss Plaintiffs’ negligence claim is denied.

2. Breach of Contract

“Under New York law, a breach of contract claim requires (1) the existence of an agreement, (2) adequate performance of the contract by the plaintiff, (3) breach of contract by the defendant, and (4) damages.” *Balk v. N.Y. Inst. of Tech.*, 683 F. App’x 89, 95 (2d Cir. Mar.

23, 2017) (summary opinion) (internal quotation marks omitted). The Complaint pleads breach of express and implied contract as separate causes of action. As detailed below, the express contract claim is dismissed, but the implied contract claim survives.

a) Breach of Express Contract

The Complaint fails to allege a sufficient claim for breach of express contract. It alleges that Plaintiffs' employment contracts "involved a mutual exchange of consideration whereby TransPerfect entrusted Plaintiffs and Class Members with particular job duties and responsibilities in furtherance of TransPerfect's services, in exchange for the promise of employment, with salary, benefits and secure PII."

The Complaint fails to allege any facts to support the conclusion that Defendant expressly contracted to protect employees' PII. The Complaint does not describe any express agreement to that effect, nor does the Complaint attach or quote any contract. In adjudicating express contract claims, "[a] court cannot supply a specific obligation the parties themselves did not spell out." *Wallert v. Atlan*, 141 F. Supp. 3d 258, 286 (S.D.N.Y. 2015) (internal quotation marks omitted). "The plaintiff must identify what provisions of the contract were breached as a result of the acts at issue." *Glob. Packaging Servs., LLC v. Glob. Printing & Packaging*, --- F.Supp.3d ----, 2017 WL 1232731, at *3 (S.D.N.Y. Mar. 31, 2017) (internal quotation marks omitted).

By failing to allege any facts upon which a finding of express contract regarding PII could be predicated, the Complaint engages in the type of "[t]hreadbare recital[] of the elements of a cause of action" that *Iqbal* warned against. 556 U.S. at 678. The second cause of action, for breach of express contract, is dismissed.

b) Breach of Implied Contract

The Complaint states a claim for breach of implied contract. “Under New York law, a contract implied in fact may result as an inference from the facts and circumstances of the case, though not formally stated in words, and is derived from the presumed intention of the parties as indicated by their conduct.” *Leibowitz v. Cornell Univ.*, 584 F.3d 487, 506–07 (2d Cir. 2009); (internal quotation marks and alterations omitted); *accord Jasper & Black v. Carolina Pad Co.*, No. 10 Civ. 3562, 2012 WL 413869, at *7 (S.D.N.Y. 2012). An implied contract, like an express contract, requires “consideration, mutual assent, legal capacity and legal subject matter.” *Id.* at 507.

Plaintiffs allege conduct and a course of dealing that raise a strong inference of implied contract. TransPerfect required and obtained the PII as part of the employment relationship, evincing an implicit promise by TransPerfect to act reasonably to keep its employees’ PII safe. TransPerfect’s privacy policies and security practices manual -- which states that the company “maintains robust procedures designed to carefully protect the PII with which it [is] entrusted” -- further supports a finding of an implicit promise. *Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015) (motion to dismiss contract claims denied based on allegation that “[d]efendants, through privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised to safeguard his PII in exchange for his employment”). *Cf. Gone v. Wackenhut Servs. Inc.*, No. 10 Civ. 2495, 2010 WL 2077210, at *2 (S.D.N.Y. May 17, 2010) (noting that limitations on an employer’s power to fire “can be found in the employment contract itself or in other employment-related documents, such as a personnel manual or employee handbook”). While TransPerfect may not have explicitly promised to protect PII from hackers in Plaintiffs’ employment contracts, “it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal

information would not imply the recipient's assent to protect the information sufficiently."

Castillo v. Seagate Tech., LLC, No. 16 civ. 1958, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016). The motion to dismiss the breach of implied contract claim is denied.

c) Damages

Defendant reframes the no-injury argument asserting the failure to plead "actual damages arising from the purported breach." The argument is unpersuasive in this context as well. As discussed above, the Complaint adequately pleads a "certainly impending" injury, as well as preventive economic injury. Similar to the tort context, the complaint alleges that Plaintiffs acted "consistent with the general contract principle[] that . . . the injured party has a duty to mitigate." *White v. Farrell*, 987 N.E.2d 244, 252 (N.Y. 2013) (internal quotation marks omitted). Plaintiffs were not legally permitted to watch passively as their identities were stolen and bank accounts drained. Consequentially, the Complaint adequately pleads all the necessary elements of breach of contract.

3. Unjust Enrichment

The claim of unjust enrichment is sufficiently pleaded. "[I]n order to adequately plead such a claim, the plaintiff must allege that (1) the other party was enriched, (2) at that party's expense, and (3) that it is against equity and good conscience to permit the other party to retain what is sought to be recovered." *Ga. Malone & Co. v. Rieder*, 973 N.E.2d 743 (N.Y. 2012) (internal quotation marks omitted). The Complaint adequately alleges all three elements -- first, that TransPerfect received the benefits of Plaintiffs' labor; second, that TransPerfect was enriched at Plaintiffs' expense when it chose to cut costs by not implementing security measures to protect Plaintiffs' PII which Defendant required or obtained in the course of Plaintiffs' employment; and third, that it would be inequitable and unconscionable to allow TransPerfect to

retain the money it saved by shirking data-security, while leaving Plaintiffs to suffer the consequences.

The unjust enrichment claim is not precluded by the contract claim. New York law “precludes unjust enrichment claims whenever there is a valid and enforceable contract governing a particular subject matter, whether that contract is written, oral, or implied-in-fact.” *Green Tree Servicing, LLC v. Christodoulakis*, 689 F. App’x 66, 71 (2d Cir. Apr. 28, 2017) (summary order). Only “where a bona fide dispute exists as to the existence of the contract, the plaintiff may proceed on both breach of contract and quasi-contract theories.” *Beth Israel Med. Ctr. v. Horizon Blue Cross & Blue Shield of N.J., Inc.*, 448 F.3d 573, 587 (2d Cir. 2006) (quoting *Nakamura v. Fujii*, 677 N.Y.S.2d 113, 116 (1st Dep’t 1998)). Here, although the Complaint adequately pleads an implied-in-fact contract, Defendant’s opposition suggests that it will dispute that Defendant agreed to be bound in an implied contract with Plaintiffs. *Accord Fero v. Excellus Health Plain, Inc.*, 236 F. Supp. 3d 735, 770 (W.D.N.Y. 2017) (declining to dismiss unjust enrichment claim where “the parties dispute whether the parties have an enforceable contract with definite and material terms regarding the provision of data security”). See generally N.Y. Pattern Jury Instr.--Civil 4:1 (“Contracts implied in fact must be distinguished from contracts implied-in-law (quasi contracts), which are not contracts at all but obligations imposed by law through the legal fiction of a contract.”).

4. N.Y. Labor Law § 203-d

Plaintiffs assert that N.Y. Labor Law § 203-d not only provides a basis for negligence per se, but also affords them a private right of action. The text of the statute is silent on private causes of action; however, that silence does not settle the issue. “In the absence of an express private right of action, plaintiffs can seek civil relief in a plenary action based on a violation of

the statute only if a legislative intent to create such a right of action is fairly implied in the statutory provisions and their legislative history.” *Nat’l Convention Servs., L.L.C. v. Applied Underwriters Captive Risk Assurance Co*, 239 F. Supp. 3d 761, 778 (S.D.N.Y. 2017) (internal quotation marks omitted). Courts decide whether a statute fairly implies a private cause of action by analyzing three factors, “of which the third is the most important: (1) whether the plaintiff is one of the class for whose particular benefit the statute was enacted; (2) whether recognition of a private right of action would promote the legislative purpose; and (3) whether creation of such a right would be consistent with the legislative scheme.” *Id.*

All three factors demonstrate that N.Y. Labor Law § 203-d implies a private right of action. First, Plaintiffs are within the class the statute is designed to protect: employees who suffered the precise type of harm that the statute is designed to prevent. Second, an implied right of action is consistent with § 203-d’s legislative purpose. In general, New York Labor Law reflects “a strong legislative policy aimed at redressing the power imbalance between employer and employee.” *Chu Chung v. New Silver Palace Rest.*, 272 F. Supp. 2d 314, 317 (S.D.N.Y. 2003) (internal quotation marks omitted). As § 203-d’s sponsor explained, the specific provision provides “important confidentiality safeguards for employees.” N.Y. Bill Jacket, 2008 S.B. 8376, Ch. 279.

Third, an implied cause of action is consistent with the legislative scheme. Section 203-d provides for administrative enforcement: the “commissioner may impose a civil penalty of up to five hundred dollars on any employer for any knowing violation” An implied private right of action is appropriate to imply in addition to administrative enforcement where “the determination of a violation and the calculation of resulting damages do not require any special agency expertise.” *Maimonides Med. Ctr. v. First United Am. Life Ins.*, 981 N.Y.S.2d 739, 748

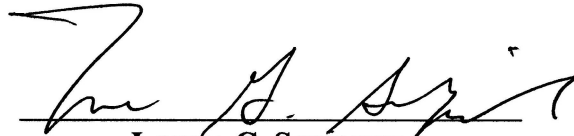
(2d. Dep’t 2014). Implied private causes of action are also especially appropriate in situations where the statute uses mandatory “shall” language.” *Id.* Here, no special agency expertise is required to determine if PII was wrongly disclosed, and the statute demands that employers “*shall* not . . . communicate an employee’s personal identifying information” N.Y. LAB. LAW § 203-d (McKinney 2009) (emphasis added). Accordingly, § 203-d implies a private right of action.

IV. CONCLUSION

For the foregoing reasons, TransPerfect’s motion to dismiss for lack of subject matter jurisdiction is DENIED. TransPerfect’s motion to dismiss for failure to state a claim is GRANTED with respect to Plaintiffs’ express contract cause of action, and otherwise DENIED. The Clerk of Court is respectfully directed to close Dkt. #20. Defendant’s request for oral argument (Dkt. 29) is DENIED as moot.

SO ORDERED.

Dated: October 4, 2017
New York, New York



LORNA G. SCHOFIELD
UNITED STATES DISTRICT JUDGE